

Remarks

The specification has been amended to add the patent numbers requested by the Examiner. The Abstract has also been amended to correct the error noted by the Examiner.

Claims 1 and 12 have been amended to recite that the cryptographic system has one of a plurality of “security-relevant” states. This is believed to have been implicit in the claims as originally presented, since the claims operate in the environment of a cryptographic system, but has been made explicit. The claims have also been amended to recite that the reply contains “nonsecret” information regarding the current state of the cryptographic system (page 35, line 7).

The Examiner asserts that the declaration does not adequately identify the specification to which it is directed and omits certain required statements (paper no. 3, ¶ 3). The filed declaration is a copy of the declaration filed with the parent application Serial No. 08/884,724, filed June 30, 1997, of which this application is a division. That declaration identifies the parent application by serial number and filing date and contains all of the statements identified by the Examiner. So the filed declaration is believed to comply with MPEP 601.01(a), and the Examiner’s objection is not understood.

The Examiner has objected to claim 12 on the ground that it is allegedly drawn to a “system”, whereas the claims dependent on claim 12 refer to “apparatus” (paper no. 3, ¶ 6). There is no inconsistency here. The preamble of 12 reads: “In a cryptographic system having one of a plurality of states, apparatus for interactively controlling the transition of said system from an existing state to a future state under control of one or more authorities” The dependent claims therefore properly refer to apparatus, since that is the subject matter of claim 12.

Claims 1-19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Taafe 4,747,139 in view of Glowny et al. 5,537,642 (“Glowny”), either alone or in combination with Schneier, Applied Cryptography (“Schneier”) (paper no. 3, ¶¶ 7 and 14).

Taaffe discloses a software security method and apparatus in which an input key 30 (Fig. 1A) is applied to a key generator 28—realized as a finite-state machine (FSM) (Fig. 2)—to generate an output key 26. An encryptor 22 uses the output key 26 to encrypt data 20 to produce encrypted data 24. The encrypted data 24 is stored along with the input key 30 on a storage medium 32. A corresponding decryption scheme is shown in Fig. 1B. The key generator 28 and an encryptor/decryptor 60, 70 are used in an otherwise conventional computer containing a CPU 50 (Figs. 6 and 7).

Analogizing Taaffe's CPU to applicants' authority and Taaffe's FSM states to applicants' cryptographic system state, the Examiner argues essentially that Taaffe discloses applicants' claimed invention except for the authentication steps. The Examiner goes on to argue that Glowny discloses these steps and that it would have been obvious to have modified Taaffe's crypto coprocessor with the teaching of Glowny of authenticating information exchanged between processors "to prevent an attacker from intercepting or changing commands being processed in route between the processors" (paper no. 3, ¶ 9). Applicants respectfully disagree.

Contrary to the Examiner's apparent assertion, Taaffe does not disclose applicants' claimed system except for the authentication steps. In applicants' claimed system, the reply provided to an authority in response to a query contains nonsecret state information regarding the current state of the cryptographic system. In Taaffe's system, on the other hand, the state of the FSM must be kept secret to ensure the security of the encryption procedure. While the Examiner refers to "status messages" provided by the FSM, applicants are unable to find any reference to such messages in the patent, and any such messages would indicate the completion of a task rather than a security-relevant state of the system as claimed by applicants.

Also, in applicants' claimed system, the request from the authority contains state change information indicating a proposed future state of the cryptographic system. In Taaffe's system, on the other hand, the internal state of the FSM, either before or after a state change, is by design secret, which the CPU can neither ascertain nor change to an arbitrary value.

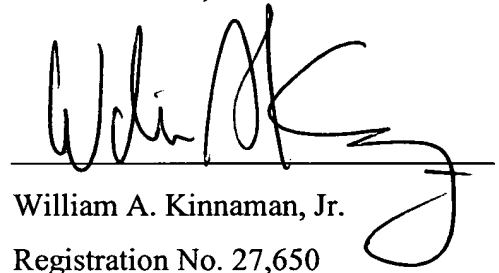
Thus even without request authentication, Taafe differs strikingly from applicants' claimed system. Accordingly, even if authentication were added as allegedly taught by Glowny, one would not obtain applicants' claimed system. Claims 1-19 as amended are therefore respectfully believed to distinguish patentably over the art cited by the Examiner.

Reconsideration of the application as amended is respectfully requested. It is hoped that upon such consideration the Examiner will hold all claims allowable and pass the case to issue at an early date. Such action is earnestly solicited.

Respectfully submitted,

RONALD M. SMITH, JR. et al.

By

A handwritten signature in black ink, appearing to read 'William A. Kinnaman, Jr.', written over a horizontal line.

William A. Kinnaman, Jr.

Registration No. 27,650

Phone: (845) 433-1175

Fax: (845) 432-9601

WAK/wak